

~~C-O-N-F-I-D-E-N-T-I-A-L~~

25X1

IBSEC-CSS-M-68

19 January 1973

COMPUTER SECURITY SUBCOMMITTEE
OF THE
UNITED STATES INTELLIGENCE BOARD
SECURITY COMMITTEE

Minutes of Meeting
Held at CIA Headquarters
Langley, Virginia
19 January 1973

1. The sixty-eighth meeting of the Computer Security Subcommittee of the United States Intelligence Board Security Committee was held on 19 January 1973 between 0930 and 1215 hours in Room 4E-64 CIA Headquarters Building. In attendance were:

[Redacted]

STAT

Major John C. Karp, Army Member
Captain Frederick R. Tucker, Air Force Member

[Redacted]

STAT

Mr. Michael F. Murphy, Treasury/USSS Member

[Redacted]

STAT

~~C-O-N-F-I-D-E-N-T-I-A-L~~

[Redacted]

25X1

C-O-N-F-I-D-E-N-T-I-A-L

25X1

STAT

2. The security level of the meeting was Top Secret SI/TK.

3. Approval of Minutes: The minutes of the 1 December and 5 January Subcommittee meetings (M-66, M-67) were approved with the following changes in the 1 December minutes:

a. Page 2, paragraph 3, first line: change "1 December" to "10 November".

b. Page 3, paragraph 4: change the second last sentence as follows: "The DIA alternate member submitted an informal proposal concerning the DIA opinions on how the COINS upgrading should be handled; a copy of this proposal is attached."

c. Provide as an attachment a copy of the informal proposal distributed at the 1 December meeting entitled, "Framework for responding to the IHC proposal for upgrading COINS".

4. Briefing on DIAOLS Security Test: As a preview for the scheduled briefings of the Security Committee and the IHC, DIA representatives presented to the Subcommittee at the instant meeting a summary of the security test of DIAOLS including its results. This briefing was presented by [redacted] It included a description of the reference points upon which the test was based, the planning of an approach to the test and evaluation process, identification of the structure of the test team, a resume of testing activities, and a summary of the conclusions. Of greatest significance was the conclusion that based on the identification of serious security weaknesses in DIAOLS as configured, it could not be accredited for compartmented operations under DCID No. 1/16. An abstract of the DIAOLS test briefing prepared by the DIA member of the Subcommittee is attached to these minutes.

STAT

C-O-N-F-I-D-E-N-T-I-A-L

25X1

C-O-N-F-I-D-E-N-T-I-A-L

25X1

5. Proposed Upgrading of COINS Security Level: At the instant meeting there was no extended discussion of the proposed COINS upgrading. However, the NSA representative affirmed that he was taking appropriate in-house action to determine whether the COINS portion of the Rye Complex could be accredited under the provisions of DCID No. 1/16. It is hoped that he will be able to provide further information on this effort at the next Subcommittee meeting. The Air Force member provided some clarification of the hardware plans for CONAD/NORAD. He indicated Air Force intention of discontinuing the use of the IBM 360/40 system as soon as possible, since the Honeywell 6050 has been delivered to the CONAD/NORAD site already.

6. In continuing the thinking of the previous Subcommittee meeting with respect to the impact of CONAD/NORAD participation in an upgraded COINS, at the instant meeting the Chairman proposed a visit to that installation by a nucleus of the Subcommittee on 16 February. He specifically expressed a need for the DIA, NSA and Air Force representatives to accompany him on such a visit in order to provide firsthand knowledge to the Subcommittee in addressing the upgrading proposal. It is expected that specific plans for this visit will be confirmed by the next meeting.

7. Planned Intelligence Community Policy Paper: The Chairman reported that in accordance with earlier tasking the Army member had developed a proposed outline for an IC computer security policy document. Notwithstanding the development of this initial outline, the Chairman suggested that Subcommittee efforts toward the development of such a policy document be modified to set aside temporarily the draft outline. Instead, the Chairman requested that members solicit from their individual organizations recommendations for specific policy items needed in the computer security field. This definition of computer security policy requirements would serve as a basis to which development of the policy document itself would respond. Members were asked to prepare written submissions in this regard for the next Subcommittee meeting.

3

C-O-N-F-I-D-E-N-T-I-A-L

25X1

C-O-N-F-I-D-E-N-T-I-A-L

25X1

8. Other Business:

a. IBM/TRW Contract: The Chairman reported that he had met with representatives of the National Bureau of Standards, the Office of the Deputy Assistant Secretary of Defense (Security Policy), and TRW Systems on 9 January to discuss coordinated Government support to the IBM/TRW contract involving computer security. At this 9 January meeting the Chairman was designated as the focal point for supporting TRW in this regard. The Government support would be provided by an ad hoc team with representatives from the Intelligence Community, the Defense Classification Community, and the balance of Government as represented by the Bureau of Standards. The earlier proposal to provide coordinated Intelligence Community support had been expanded to include the other Government environments, as a result of the Chairman's discussions with TRW in December 1972 and a solicitation to become involved on the part of the Director, Institute for Computer Sciences and Technology, National Bureau of Standards.

The Chairman informally opined that this ad hoc team would be made up of approximately six representatives of each environment. At the instant meeting the Army and Treasury representatives indicated that they would not participate in an active fashion. USIB participation is expected on the part of at least CIA, DIA, NSA, and AEC. Members were told to identify by the end of January 1973 an individual in those member organizations where active participation is expected.

b. IHC Proposal for Computer Security Procedures Handbook: For the information of members and discussion with their IHC counterparts, the Chairman called to the Subcommittee's attention a proposal being entertained

C-O-N-F-I-D-E-N-T-I-A-L

25X1

C-O-N-F-I-D-E-N-T-I-A-L

25X1

by the IHC to develop on an expedite basis through the assignment on a full-time basis of representation from various USIB agencies of a Computer Security Procedures Handbook. He expressed his own view, as concurred in by the Chairman of the Security Committee, that development of such a Handbook should be deferred until the current Subcommittee action is completed on the development of an Intelligence Community computer security policy paper.

c. SECOM Visit to IBM: The Chairman informed Subcommittee members that he had arranged for a presentation on computer technology for the Security Committee at the IBM Washington Presentation Center to take place on 13 February 1973. He asked Subcommittee members to encourage their Security Committee principals to attend this presentation.

d. Data Sentinel Presentation: At the instant meeting the DIA representative extended an invitation to member organizations to attend a briefing on the Data Sentinel computer security system, scheduled to be given at 0900 hours on 2 February by the manufacturer, Basic Computing Arts Inc., Palo Alto, California. Members were asked to submit the names of attendees to DIA in advance of the scheduled presentation. (The date and time of this presentation was subsequently changed to 23 February at 1330 - 1530 hours.

e. OSD (Security Policy) Participation in CSS Activities: The Chairman noted recent telephonic contact with the Office of the Deputy Assistant Secretary of Defense (Security Policy) in which a representative of that office suggested the possibility of his participation in meetings of the Computer

C-O-N-F-I-D-E-N-T-I-A-L

25X1

C-O-N-F-I-D-E-N-T-I-A-L

[REDACTED]

25X1

Security Subcommittee. The suggestion was based on newly assigned responsibilities of that office under the new DOD directive on computer security (5200.28). The Chairman expressed no personal opposition to this suggestion, but requested the DIA representative to investigate the protocol considerations involved. Following report from the DIA member, the Chairman may propose to the Security Committee that representation in observer status be extended to the Office of DASD(SP).

9. The next Subcommittee meeting was scheduled for 9 February 1973 at 0930 hours.

[REDACTED]

STAT

Chairman
Computer Security Subcommittee

C-O-N-F-I-D-E-N-T-I-A-L

[REDACTED]

25X1

C-O-N-F-I-D-E-N-T-I-A-L

DIAOLS TEST BRIEFING

ABSTRACT

The purpose of the briefing was to describe the conduct, results and potential implications of the Multi-Level Security Analysis, Test and Evaluation of the DIA On-Line System (DIAOLS). The test background, going back to 1969, was described as stemming from the test and evaluation of the predecessor DIA system, the Analyst Support and Research System (ANSRS), wherein multi-level security was envisioned as feasible on ANSRS and desirable from two points of view: it would enhance system effectiveness by incorporating SAO material, and at the same time, additional users and terminals could be added to the system at reduced security costs. The test significance included the following: it was the first intensive, comprehensive ADP system test wherein all facets of the security subsystem were tested; in methodology, the effort represented the simulation of a hostile attack; and the overall effort essentially represented a two-fold hypothesis: that multi-level security was feasible in terms of contemporary technology, and that DIAOLS was the model for implementing a multi-level capability.

The formal objective of the test was also two-fold: to determine accreditation/non-accreditation of the DIAOLS for the "Compartmented Mode of Operation", and to gain experience and develop methodologies in the security analysis, test and evaluation of resource-sharing computer systems in order to validly and effectively implement DCID No. 1/16 within the Department of Defense. The basic policy framework for test conduct was reviewed, including the definition of "Compartmented Mode of Operation", the pertinent provisions of DCID No. 1/16, with amplifying guidelines, and the DIA test approach involving contractor/consultants and outside participation in the interests of test credibility and objectivity.

As a result of the effort, the test team concluded that the DIAOLS system was in a state of significant security vulnerability

C-O-N-F-I-D-E-N-T-I-A-L

C-O-N-F-I-D-E-N-T-I-A-L

due to both its technical hardware/software inadequacies and deficiencies in physical/procedural security practices. Because of the design and implementation vulnerabilities in the system software together with the programming capabilities offered to users, the test team was able to clandestinely acquire unauthorized access to user identifiers, authenticators and other information, thereafter giving them unrestricted access to the total system, including unauthorized access to COINS files. The overall problem was rooted in the basic operating system, GCOS III; accordingly, the team did not feel that "patched" software corrections to the system were an adequate solution. They, therefore, recommended against accreditation of the DIAOLS. Positive recommendations in the technical area revolved around segregation of the programming capabilities on one of the two DIAOLS cpu's and placing the intelligence files with a separate set of authenticators on the other cpu. The latter system, following further testing, may be accreditable for the compartmented mode.

Limitations in the validity and effectiveness of both methodology and criteria were suggested; however, it was concluded that no viable alternatives existed for at least the near-term future. Limitation of the test activity to attacks through the programming languages only was also noted, suggesting that further effort to investigate the security posture of systems not offering such capabilities to users was highly desirable.

Overall, the test results suggested that security considerations would emerge as a more complex constraint in applying advanced ADP technology to processing information handling tasks over the near term than had been expected. The extent of these constraints would have to be determined by future experience, particularly through additional testing. It was indicated that future computer security policy efforts must be directed toward the specification of a meaningful operation definition of "acceptable level of risk" along with a reasonable set of specific application criteria. Concurrently, a continued R&D effort by both Government and private industry to develop a "secure" computer system must be strongly encouraged.

C-O-N-F-I-D-E-N-T-I-A-L